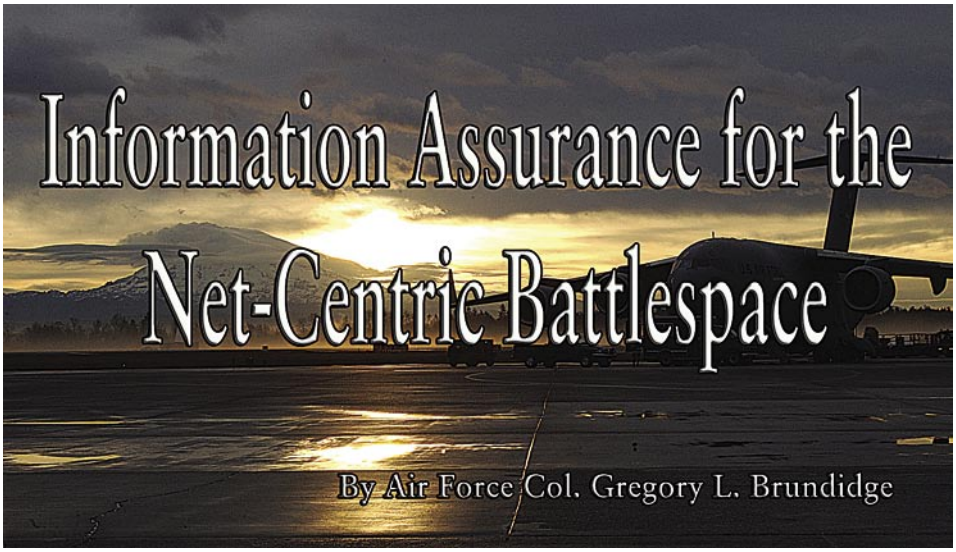

To meet the demands of today's net-centric-operations environment or battlespace, we must adapt a much broader construct for information assurance …

Today's aerospace operations environment is highly complex, lethal, and one that we must continue to dominate to achieve military operational objectives. Central to achieving these operational ends are the concepts of vertical and horizontal integration. These two operational tenets form the basis for how processes, operational capabilities and decision-quality information flow are knitted together to minimize or eliminate seams in the find-fix-target-track-engage-assess-kill chain.

Our recent successes in air campaigns in the Balkans and Southwest Asia demonstrate how well we have mastered the art and science of aerospace operations. Aerospace dominance, time-sensitive targeting, predictive battlespace awareness and effects-based operations are now today's essential operational realities.

Looking forward, we must further evolve these realities to achieve total battlespace awareness supporting real-time decision-making. Total battlespace awareness depends on dominant and agile operational support from a capabilities-focused enterprise that meets warfighter needs and eliminates seams.

At the center of all of these major operational movements is "the net" — the aggregate of all network connectivity (terrestrial, airborne and space), capabilities and processes from the physical layer connections and protocols, to net-enabled operational processes and applications. It is the essential fabric that serves to integrate vertically and horizontally, facilitates battlespace awareness and effects-based operations, enables operations support from a capability-focused enterprise and provides the means for accurate real-time decisions.

In this net-centric environment, information assurance is not simply ensuring that information is protected, accurate and delivered on time, it also means ensuring that all the components involved in making that happen are postured, prepared and ready to do so.

To define IA requirements for the net-centric environment, we must consider three pillars:

•**Technology:** Relevant technical capabilities and mission-driven innovation.

•**Processes:** Concept of Operations (CONOPS) and tactics, techniques and procedures (TTPs).

•**People:** Indoctrination, Training and Development.

Technology

When we consider the unstoppable advance of increasing capabilities in information processing, transfer and networking, the essential first component for IA is capable technology. As industry continues to improve information technology capabilities to process, exchange, transfer and store more information, faster and better, we must demand the parallel development of information protection capabilities. The ability to achieve authentication, integrity, confidentiality, non-repudiation and availability, the traditional elements of information assurance, or what we call "small ia," relies heavily on technologies that are on par with advancing information capabilities.

Therefore, it is not only important for us to be competent with today's ia technologies, but we must always have an eye on the ia technologies for tomorrow. Encryption, intrusion detection, firewall and authentication tools for our networks must evolve and grow with other network capabilities. This is especially important as more and more of these technologies are designed into network components vice stand-alone, add-on boxes.

By staying in touch with those who perform network operations (NETOPS) and deliver the full spectrum of network services, those who acquire these capabilities for the Air Force and Department of Defense (DoD) can ensure they deliver timely, usable and relevant technologies for tomorrow's ia demands.

Equally as important, is the need to standardize on vendor solutions or, at a minimum, provide specifications for vendors to meet when providing hardware or software components for the net-centric environment. This is an essential step to eliminating hard-to-manage, service disruptions on our networks and corresponding training and operations and management challenges in our NETOPS centers.

We do not acquire other weapon systems this way, so we should not expect our air crews and air, space and missile operators to train for unmanaged variability in the systems they operate.

Processes

We must consider the other two essential components: *processes and people*. To effectively command and control net-centric operations there must be well-defined

CONOPS, policies and procedures for governance, operation and sustainment.

Because NETOPS in the net-centric environment is a young operational discipline, we are in the process of developing many of the governing and guiding documents. Several CONOPS, such as the Air Force Network Operations (AFNETOPS), Air Force Network Operations Security Center (AFNOSC or Global NETOPS) and Integrated-Network Operations and Security Center (I-NOSC) have been finalized or are in draft review.

Likewise, we continue to evolve policy and strategy documents for guiding the development, implementation and operation of the net.

The process component of what we call "big IA" is critical because it enables optimized use of available technological capabilities. It does no good to have superior information technology — if we don't have the processes in place that enable us to leverage its power and transform it into relevant operational capability for the warfighter.

How often have we raced to field the latest hardware or software network tool or application only to complete fielding and find that we did not evolve our operations, concepts and procedures, so that our net technicians and users could leverage full capability?

Instead, we must use a capability-driven model that brings new network capabilities as operational requirements dictate and adjust CONOPS and associated processes and procedures prior to fielding. Ideally, we should train our technicians in advance, so we can implement new capabilities without disrupting current NETOPS.

The Air Force transitioned from SCOPE Network teams that focused on optimizing and securing base networks to SCOPE EDGE (enterprise, design, guidance and evaluation) teams. The advent of a centralized standardization and evaluation program, such as SCOPE EDGE for NETOPS, is a critical first step to form the foundation of a broader standardization and evaluation construct that will assess all critical processes delivering the net-centric environment. This will include network management, network administration, network defense and associated NOSC and Network Control Center (NCC) operations.

We will know we have achieved success when the TTPs, checklists, bold print and technical orders (TO) that govern these processes are in place and guiding the actions on the operations floors of our NETOPS centers. To keep these items current, the process for evolving network capability must accommodate the steps necessary to update them as we add new tools, applications and capabilities.

People

The most important component of the big IA triad is our people. It is our people who deliver the net-centric environment today in a less than ideal environment. We made a significant step in improvement with the advent of the Operationalizing and Professionalizing the Network (OPTN) initiative in 1998 to treat the network as a weapons system as one base, one network and one enclave.

However, with the exception of a recurring funded training line for essential network skills and standard NCC structures, we stopped short of realizing the OPTN objectives of an operationalized NOSC, NCC, and a professionally-certified and mission-qualified force of network technicians.

In the net-centric environment, the essential mindset is one that understands the interdependencies of the net and fully appreciates the importance of standards in our technologies and processes. The transformed net professional realizes that a network risk or vulnerability assumed by one is assumed by all. To complete a necessary mindset transformation, we start with training processes that span the development cycle for the technician.

From technical school to 7-level training, the program must be focused on building cross-trained net technicians. If we have standard system hardware and applications, and we employ standard processes and procedures in our NOSCs, NCCs and other NETOPS centers, then we should be able to mission-qualify and certify crew members who can perform proficiently in a like crew position at any Air Force NCC or NOSC.

We should "push the envelope" wherever possible to take net warrior training to the next level …

In addition to standardized training, we should "push the envelope" wherever possible to take net warrior training to the next level.

In industry, credibility comes from not only being able to deliver capabilities upon demand, but also from the level of certification one brings to the table. Thus, along with baseline training that allows net warriors to seamlessly flow from one organization to another, we should work toward getting our people mission-driven certifications recognized by industry, and focus on higher degrees of mission qualifications.

Certifications, such as Certified Information Systems Security Professional, Project Management Professional and Security A+, could equate to specialist, senior specialist and master specialist ratings for NCC and NOSC crew positions. Ratings would be determined by training and education completed, hours in the position and scores on check rides.

These ratings would mark the difference between those who dabble in our field and those whom we would consider to be experts. This produces a win-win situation for our organizations and the individual. Additionally, it raises the bar for improving net-centric operations across all dimensions of the mission area.

We can and must take steps to achieving a standard environment and training. As we standardize hardware and software and the TTPs we use to employ them, we pave the way for completing a transformation. To succeed, we must have the flexibility and leeway to acquire standard infrastructure hardware and core service applications for the Air Force.

Air Force Col. Gregory L. Brundidge is the former director of Communications and Information Pacific Air Forces. CHIPS